#2

PATENT
81942.0011
Express Mail Label No. EL 713 695 963 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Junichi MURAKAMI	Examiner: Not assigned
Serial No: Not assigned	
Filed: January 22, 2001	
For: COMMON KEY GENERATING METHOD, COMMON KEY GENERATOR, CRYPTOGRAPHIC COMMUNICATION METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM	

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016362 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 22, 2001

By:_____
Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　１月２５日

出 願 番 号
Application Number: 特願２０００－０１６３６２

出 願 人
Applicant (s): 村田機械株式会社
笠原　正雄

２０００年　８月１８日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号　出証特２０００－３０６４８４４

【書類名】　特許願

【整理番号】　20907

【提出日】　平成12年 1月25日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00

G09C 1/00

【発明の名称】　共通鍵生成方法、共通鍵生成器、暗号通信方法、暗号通信システム及びプログラムを記録した記録媒体

【請求項の数】　11

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【復代理人】

【識別番号】　100114557

【弁理士】

【氏名又は名称】　河野　英仁

【電話番号】　06-6944-4141

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　共通鍵生成方法、共通鍵生成器、暗号通信方法、暗号通信システム及びプログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする共通鍵生成方法。

【請求項２】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項１に記載の共通鍵生成方法。

【請求項３】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成器において、通信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段を備えることを特徴とする共通鍵生成器。

【請求項４】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項３に記載の共通鍵生成器。

【請求項５】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成

した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする暗号通信方法。

【請求項６】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項５に記載の暗号通信方法。

【請求項７】

前記センタは複数有り、複数の各センタが各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を発行することを特徴とする請求項５又は６に記載の暗号通信方法。

【請求項８】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信システムにおいて、各エンティティには、通信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段と、を備えたことを特徴とする暗号通信システム。

【請求項９】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項８に記載の暗号通信システム。

【請求項１０】

コンピュータに、センタから送付された各エンティティ固有の秘密鍵と通信相手のエンティティの特定情報とから暗号通信に利用する共通鍵を生成させるため

のプログラムが記録されているコンピュータ読み取りが可能な記録媒体において、通信相手のエンティティの特定情報の構成要素に不足があるどうかの判断をコンピュータに実行させる第１プログラムコード手段と、前記通信相手のエンティティの特定情報の構成要素に不足があると判断された場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成させることをコンピュータに実行させる第２プログラムコード手段と、を含むことを特徴とするプログラムが記録されている記録媒体。

【請求項１１】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項１０に記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、エンティティ間の暗号通信に利用される共通鍵を生成する共通鍵生成方法、共通鍵生成器、エンティティ間で暗号通信を行う暗号通信方法、暗号通信システム、及びそれらに用いられるプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換するこ

とである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号方式は、共通鍵暗号方式と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standard）はその典型例である。このような共通鍵暗号方式の従来例は、次のような３種の方法に分類できる。

【０００５】

①　第１の方法

暗号通信を行う可能性がある相手との共通鍵をすべて秘密保管しておく方法。

②　第２の方法

暗号通信の都度、呼び通信により鍵を共有し合う方法（Diffie-Hellmanによる鍵共有方式、公開鍵方式による鍵配送方式等）。

③　第３の方法

各ユーザ（エンティティ）の氏名、住所等の個人を特定する公開された特定情報（ＩＤ（Identity）情報）を利用して、予備通信を行うことなく、送信側のエンティティ、受信側のエンティティが独立に同一の共通鍵を生成する方法（ＫＰＳ（Key Predistribution System）、ＩＤ－ＮＩＫＳ（ID-based Non-Interactive Key Sharing Schemes）等）。

【０００６】

第１の方法では、通信相手の共通鍵を保管しておく必要がある。また、第２の方法は、鍵共有のための予備通信が必要である。第３の方法は、通信相手の共通鍵を保管する必要もなく、予備通信も不要であり、公開された相手のＩＤ情報と

センタから予め配布されている固有の秘密パラメータとを用いて、必要時に、任意の相手との共通鍵を生成できるので、便利な方法である。

【０００７】

図１１は、このＩＤ－ＮＩＫＳのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図１１において、エンティティＸの特定情報であるエンティティＸの名前、住所、電話番号等のＩＤ情報は、ハッシュ関数ｈ（・）を用いてｈ（ID_X）で表す。センタは任意のエンティティＸに対して、センタ公開情報｛PC_i｝、センタ秘密情報｛SC_i｝及びエンティティＸのＩＤ情報ｈ（ID_X）に基づいて、以下のように秘密鍵S_{Xi}を計算し、秘密裏にエンティティＸへ配布する。

$$S_{Xi}=F_i(\{SC_i\},\ \{PC_i\},\ h(ID_X))$$

【０００８】

エンティティＸは他の任意のエンティティＹとの間で、暗号化、復号のための共通鍵K_{XY}を、エンティティＸ自身の秘密鍵｛S_{Xi}｝、センタ公開情報｛PC_i｝及び相手先のエンティティＹのＩＤ情報ｈ（ID_Y）を用いて以下のように生成する。

$$K_{XY}=f(\{S_{Xi}\},\ \{PC_i\},\ h(ID_Y))$$

また、エンティティＹも同様にエンティティＸへの共通鍵K_{YX}を生成する。もし常に$K_{XY}=K_{YX}$の関係が成立すれば、この鍵K_{XY}，K_{YX}をエンティティＸ，Ｙ間で暗号化鍵、復号鍵として使用できる。

【０００９】

本発明者等は、このようなＩＤ－ＮＩＫＳについて種々の暗号化方法、共通鍵生成方法、暗号通信方法等を提案しており、また、各エンティティのＩＤ情報を複数に分割して複数の各センタからその分割ＩＤ情報に基づく秘密鍵をエンティティに配布する構成にして、より安全性を高めるようにしたＩＤ－ＮＩＫＳによる暗号化方法、共通鍵生成方法、暗号通信方法等についても、提案している。

【００１０】

上記提案においては、ＩＤ情報として電子メールアドレスを使用し、各エンティティにおいて共通鍵を生成する際、各エンティティは各センタから発行された

各エンティティ固有の秘密鍵と通信相手となるエンティティの電子メールアドレスに基づいて、共通鍵を生成する。その共通鍵を使用して、送信時には平文を暗号化して暗号文を生成し、受信時には暗号文を復号して平文を再生する。

【００１１】

【発明が解決しようとする課題】

各エンティティが、ドメイン名が付いている電子メールアドレスを自己の電子メールアドレスとして、秘密鍵登録を行っていると、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、共通鍵を正しく生成できないので、暗号通信を行うことができなくなる。

【００１２】

本発明は斯かる事情に鑑みてなされたものであり、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合でも、確実に共通鍵を生成できる共通鍵生成方法及び暗号通信方法等を提供することを目的とする。

【００１３】

【課題を解決するための手段】

本発明の共通鍵生成方法においては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする。

【００１４】

また、本発明の共通鍵生成器においては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成器において、通

信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段を備えることを特徴とする。

【００１５】

また、本発明の暗号通信方法においては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする。

【００１６】

また、本発明の暗号通信システムにおいては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信システムにおいて、各エンティティには、通信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段と、を備えたことを特徴とする。

【００１７】

また、本発明のコンピュータ読み取りが可能な記録媒体においては、コンピュータに、センタから送付された各エンティティ固有の秘密鍵と通信相手のエンティティの特定情報とから暗号通信に利用する共通鍵を生成させるためのプログラ

ムが記録されているコンピュータ読み取りが可能な記録媒体において、通信相手のエンティティの特定情報の構成要素に不足があるどうかの判断をコンピュータに実行させる第１プログラムコード手段と、前記通信相手のエンティティの特定情報の構成要素に不足があると判断された場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成させることをコンピュータに実行させる第２プログラムコード手段と、を含むことを特徴とする。

【００１８】

また、上記の発明において、前記特定情報は電子メールアドレスであり、前記構成要素の一部はドメイン名であることを特徴とする。

【００１９】

また、上記の発明において、前記センタは複数有り、複数の各センタが各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を発行することを特徴とする。

【００２０】

本発明では、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、自己の電子メールアドレスのドメイン名と同じドメイン名を、相手の電子メールアドレスに付けてから共通鍵を生成するので、確実に共通鍵を生成することができる。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（Ｋ個）のセンタ１が、秘密鍵発行のサーバとして設定されている。なお、これらのセンタ１としては、例えば社会の公的機関を想定できる。

【００２２】

これらの各センタ１と、この暗号通信システムを利用するユーザとしての複数の各エンティティａ，ｂ，‥，ｚとは、通信路2_{a1}，‥，2_{aK}、2_{b1}，‥，2_{bK}、・・・、2_{z1}，‥，2_{zK}により接続されており、これらの通信路を介して、各

エンティティａ，ｂ，‥，ｚから各センタ１へ秘密鍵発行の依頼がなされ、各センタ１から各エンティティ固有の秘密鍵が各エンティティａ，ｂ，‥，ｚへ発行されるようになっている。また、２人のエンティティ間には電子メールによる通信路3_{ab}，3_{az}，3_{bz}，‥が設けられており、通信情報を暗号化した暗号文が互いのエンティティ間で電子メールにより送受信されるようになっている。

【００２３】

図２は、２人のエンティティａ，ｂ間における情報の通信状態を示す模式図である。図２の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ送信し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００２４】

総数Ｋ個の各センタ１には、自身の秘密情報（対称行列）から各エンティティａ，ｂ毎に選択したものを各エンティティのパスワードに基づいて暗号化して各エンティティａ，ｂ固有の秘密鍵を発行する秘密鍵発行器２が備えられている。秘密鍵発行器２は、その内部構成を示す図３に表すように、暗号化された秘密情報を格納する秘密情報格納部３と、秘密情報格納部３に格納されている暗号化秘密情報を読み出して復号する秘密情報復号部４と、センタ１自身の秘密情報と各エンティティａ，ｂの特定情報（ＩＤ情報）から各エンティティａ，ｂ固有の秘密鍵を作成する秘密鍵作成部５と、作成された秘密鍵を各エンティティａ，ｂから入力されたパスワードで暗号化する秘密鍵暗号化部６と，所定周期毎に更新されるセンタ１の秘密情報を暗号化して秘密情報格納部３に書き込む秘密情報更新部６とを有する。

【００２５】

エンティティａ側には、Ｋ個の各センタ１に対して秘密鍵の発行を要求する登録部１０と、Ｋ個の各センタ１から送られる秘密鍵方式でのエンティティａ自身固有の秘密鍵を復号する第１秘密鍵復号部１１と、復号されたＫ個の自身固有の秘密鍵を暗号化する秘密鍵暗号化部１２と、暗号化された秘密鍵を格納する秘密鍵格納部１３と、秘密鍵格納部１３に格納されている暗号化秘密鍵を読み出して復号する第２秘密鍵復号部１４と、自身固有の秘密鍵とエンティティｂの特定情

報（ＩＤ情報）とに基づいてエンティティａが求めるエンティティｂとの共通鍵K_{ab}を生成する共通鍵生成部１５と、共通鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して電子メールによる通信路３０へ出力する平文暗号化部１６と、共通鍵、平文、暗号文等を表示する表示部１７とが備えられている。

【００２６】

また、エンティティｂ側には、Ｋ個の各センタ１に対して秘密鍵の発行を要求する登録部２０と、Ｋ個の各センタ１から送られる秘密鍵方式でのエンティティｂ自身固有の秘密鍵を復号する第１秘密鍵復号部２１と、復号されたＫ個の自身固有の秘密鍵を暗号化する秘密鍵暗号化部２２と、暗号化された秘密鍵を格納する秘密鍵格納部２３と、秘密鍵格納部２３に格納されている暗号化秘密鍵を読み出して復号する第２秘密鍵復号部２４と、自身固有の秘密鍵とエンティティａの特定情報（ＩＤ情報）とに基づいてエンティティｂが求めるエンティティａとの共通鍵K_{ba}を生成する共通鍵生成部２５と、共通鍵K_{ba}を用いて通信路３０から入力した暗号文Ｃを平文（メッセージ）Ｍに復号して出力する暗号文復号部２６と、共通鍵、平文、暗号文等を表示する表示部２７とが備えられている。

【００２７】

次に、このような構成の暗号通信システムにおける暗号通信の処理動作について説明する。

【００２８】

（予備処理）

各エンティティを特定する特定情報（ＩＤ情報）、例えばそのエンティティの電子メールアドレスを表すＩＤベクトル（Ｌビット２進ベクトル）を、図４に示すように、ブロックサイズＭビット毎にＫ個のブロックに分割する。例えば、エンティティａの電子メールアドレスを示すＩＤベクトル（ベクトルI_a）を式（１）のように分割する。分割特定情報である各ベクトルI_{aj}（ｊ＝１，２，・・・，Ｋ）を分割ＩＤベクトルと呼ぶ。なお、エンティティの電子メールアドレスが、ハッシュ関数によってＬビットのＩＤベクトルに変換される。

【００２９】

【数１】

$$\overrightarrow{I_a} = [\overrightarrow{I_{a1}} | \overrightarrow{I_{a2}} | \cdots | \overrightarrow{I_{aK}}] \quad \cdots (1)$$

【００３０】

（秘密鍵発行処理（エンティティの登録処理））

図５及び図６に、エンティティａ，ｂの登録部１０、２０によるセンタへの登録処理及び、各センタ１の秘密鍵発行器２による秘密鍵発行処理を示す。この暗号通信システムに参加したいエンティティａ，ｂ、即ち、自身固有の秘密鍵の発行を希望するエンティティａ，ｂは、各センタ１（センタ第１、第２、・・、第Ｋ）へ登録し、秘密鍵を入手する。

【００３１】

まず、図５（Ｉ）に示すように、エンティティａでは、基本パスワードと自身の電子メールアドレスを登録部１０へ入力する（Ｓ１１１）。登録部１０は、基本パスワードと一方向性変換関数に基づいて、センタ第１用のパスワードを生成し（Ｓ１１２）、センタ第１への登録処理を行い、センタ第１から秘密鍵を入手する（Ｓ１１３）。

【００３２】

同様に、それぞれ異なる一方向性変換関数を用いて、センタ第２用、センタ第Ｋ用のパスワードを生成し、センタ第２、センタ第Ｋへの登録処理を行い、秘密鍵を入手する（Ｓ１１４～Ｓ１１７）。同様に、図５（II）に示すように、エンティティｂにおいても、登録部２０により各センタ１への登録処理を行い、各センタ１から秘密鍵を入手する（Ｓ１２１～１２７）。

【００３３】

次に、図６を参照しながら、エンティティａにおけるセンタ第１への登録処理及びセンタ第１におけるエンティティａの秘密鍵発行処理について説明する。他のエンティティにおける登録処理及び他のセンタにおける秘密鍵発行処理についても同様である。

【００３４】

エンティティａの登録部１０では、Ｓ１１２で生成されたセンタ第１用のパス

ワードを取り込み（Ｓ２１１）、センタ第１のホームページにアクセスしてサーバを介して、パスワードとエンティティａ自身の電子メールアドレスとを公開鍵方式（ＳＳＬ等）で暗号化しセンタ第１へ送信する（Ｓ２１２，Ｓ２１３）。

【００３５】

センタ第１の秘密鍵発行器２では、秘密情報格納部３に格納されている暗号化秘密情報を秘密情報復号部４で復号した秘密情報（後述する対称行列）を得る（Ｓ２２１）。また、エンティティａから公開鍵方式で暗号化されたパスワードと電子メールアドレスを受信し（Ｓ２２２）、復号する（Ｓ２２３）。秘密鍵作成部５にて、エンティティａの電子メールアドレスから得られた分割ＩＤベクトルに対応する部分を選択し、エンティティａの秘密鍵（後述する秘密鍵ベクトル）を生成する（Ｓ２２４）。

【００３６】

生成した秘密鍵（秘密鍵ベクトル）をエンティティａから受信したパスワードに基づいて暗号化して（Ｓ２２５）、即ち、選択した秘密鍵（秘密鍵ベクトル）にパスワードを盛り込んだ秘密鍵方式で、そのエンティティ固有の秘密鍵を、電子メールを介してそのエンティティに発行する（Ｓ２２６）。この際の秘密鍵方式としては、ＤＥＳを利用できる。なお、エンティティの電子メールアドレスを暗号化して送付するようにしても良い。

【００３７】

エンティティａは、暗号化されたエンティティａの秘密鍵（秘密鍵ベクトル）を受信し（Ｓ２１４）、パスワードを用い、第１秘密鍵復号部１１で復号する（Ｓ２１５）。さらに、復号した秘密鍵（秘密ベクトル）は安全のため、一旦、秘密鍵暗号化部１２で暗号化されて（Ｓ２１６）、秘密鍵格納部１３に格納される。

【００３８】

同様にしてエンティティａは、センタ第２、・・、第Ｋへ登録を行い、秘密鍵を入手する。上述のように、各センタ１によって発行された各エンティティの秘密鍵（秘密鍵ベクトル）は、パスワードによって各センタ１で暗号化されてから各エンティティへ送付され、各エンティティで復号されるので、各エンティティ

は秘密鍵（秘密鍵ベクトル）を秘密裡に入手することができる。

【００３９】

安全のためには、各センタ１毎にそれぞれ固有のパスワードを送付することが望ましいが、パスワードの管理が煩雑になる可能性がある。そこで、１つの基本パスワードと一方向性変換関数に基づいて、複数のパスワードを生成することにより、管理が必要なパスワード数を削減することができる。また、一方向性変換関数を秘密にすることにより、安全性が損なわれることはない。

【００４０】

１つの基本パスワードと一方向性変換関数に基づいて複数のパスワードを生成するには、次のような方法がある。

①各センタ１毎に異なる一方向性変換関数を使用する。

②基本パスワードに各センタ毎に異なるスクランブル処理を施したり、各センタ毎に連番を付加するなどしてから、各センタ１で共通又は各センタ１毎に異なる一方向性変換関数を使用する。

【００４１】

また、一方向性変換関数として一方向性ハッシュ関数を用いることができる。一方向性ハッシュ関数による演算後のパスワードは、元の基本パスワードよりデータ長が短くなるので、不都合であれば、適宜、異なる複数の一方向性ハッシュ関数による演算結果を組み合わせてパスワードを構成する。このようにすれば、一方向性ハッシュ関数による、データ長の低減を補うことができる。

【００４２】

なお、より簡易的に、電子メールにより、エンティティの登録処理及び秘密鍵の発行処理を行うことも可能である。この場合、自身固有の秘密鍵の発行を希望するエンティティは、自身のパスワードを電子メールにて直接各センタ１へ公開鍵方式で送る。各センタ１では、上記の場合と同様に、秘密情報からエンティティに対応して選択した秘密鍵にエンティティ側で入力されたパスワードを盛り込んだ秘密鍵方式（ＤＥＳ等）でそのエンティティ固有の秘密鍵を、電子メールを介してそのエンティティに発行する。

【００４３】

なお、上述した例では、電子メールにて秘密鍵を発行するようにしているが、ＩＣカード等の可搬型の記録媒体にエンティティ固有の秘密鍵を書き込み、その記録媒体をエンティティへ送るようにすることも可能である。

【００４４】

ここで、各センタ１での秘密情報（対称行列）、及び、各エンティティ固有の秘密鍵（秘密鍵ベクトル）の具体的内容について説明する。ｊ（ｊ＝１，２，・・・，Ｋ）番目のセンタ１は、秘密情報として、ランダムな数を要素とする対称行列H_j（$2^M \times 2^M$）を有している。そして、エンティティａに対して、対称行列H_jのそのエンティティの分割ＩＤベクトルに対応する行ベクトルを秘密鍵（秘密鍵ベクトル）として発行する。即ち、エンティティａに対しては、H_j〔ベクトルI_{aj}〕を発行する。このH_j〔ベクトルI_{aj}〕は、対称行列H_jよりベクトルI_{aj}に対応した行を１行抜き出したベクトルを表す。

【００４５】

ここで、エンティティ側でのパスワード入力の例について説明する。パスワード入力処理については、パスワード入力が不慣れなエンティティにとって特に、次のような２つの例が好適である。

【００４６】

一方の例では、各エンティティが文字列を入力し、その入力データをｂａｓｅ６４でエンコードしたものをパスワードとする。この場合、６４種の各１つの文字入力にて６ビットのデータを表せるので、パスワードが６４ビットである場合には、１１個の文字を入力すれば良いことになる。

【００４７】

また、他方の例では、０～９及びＡ～Ｆの１６種の文字を入力することを原則として、これらの１６種の文字以外が入力された場合には、その文字を０～９，Ａ～Ｆの何れかの文字に置換する。

【００４８】

（エンティティａ，ｂにおける共通鍵の生成処理）

エンティティａ，ｂにおける共通鍵生成処理について、図７を参照しながら説明する。エンティティａ（エンティティｂ）は、通信相手であるエンティティｂ

（エンティティａ）との共通鍵K_{ab}（K_{ba}）を生成する際に、暗号化された秘密鍵（秘密鍵ベクトル）を秘密鍵格納部１３（２３）から読み出して、第２秘密鍵復号部１４（２４）で再び秘密鍵（秘密鍵ベクトル）を復号する（Ｓ３１１（Ｓ３２１））。

【００４９】

エンティティａ（エンティティｂ）は、共通鍵を生成するために相手のエンティティｂ（エンティティａ）の特定情報（ＩＤ情報）としての電子ｆを必要とする。送信側となるエンティティａにおいては、エンティティｂの電子メールアドレスは送信相手先の電子メールアドレスとして与えられる。また、受信側となるエンティティｂにおいては、エンティティａの電子メールアドレスは受信した電子メールの発信元情報（Ｆｒｏｍフィールド等）から得ることができる（Ｓ３２２）。

【００５０】

共通鍵生成部１５（２５）にて、各センタ１から受け取った秘密鍵（秘密鍵ベクトル）のうち、エンティティｂ（エンティティａ）の特定情報（ＩＤ情報）に基づいて、対応する要素を取り出し、これらＫ個の要素を合成して、エンティティａ（エンティティｂ）のエンティティｂ（エンティティａ）に対する共通鍵K_{ab}（K_{ba}）を生成する（Ｓ３１２（Ｓ３２３））。ここで、Ｋ個の各センタが有する秘密情報（行列）の対称性に基づいて、両共通鍵K_{ab}，K_{ba}は一致する。

【００５１】

エンティティａ，ｂの特定情報（ＩＤ情報）として、電子メールアドレスを利用している。図８に示すように、電子メールアドレスはメールシステムによって、ドメイン名が付いているもの（図８（Ｉ））と、付いていないもの（図８（II））がある。ドメイン名が付いている電子メールアドレスはインターネットの電子メールアドレスとして使用されている。また、インターネット以外のメールシステムにおいては、ドメイン名が付いていない電子メールアドレスを使用していることもある。

【００５２】

ゲートウェイを介してインターネットに接続されたＬＡＮ環境においては、こ

れら２種類の電子メールアドレスのいずれでも使用できる場合がある。例えば、ＬＡＮなどの閉じた範囲では、いずれの電子メールアドレスでも使用可能であり、ゲートウェイを介してインターネットメールを使用する場合には、ドメイン名が付いている電子メールアドレスを使用するようになっている。

【００５３】

エンティティａ，ｂにおいては、インターネットの電子メールにより、各センタから秘密鍵（秘密鍵ベクトル）を入手した場合には、ドメイン名が付いている電子メールアドレスに基づいて秘密鍵（秘密鍵ベクトル）が生成されている。したがって、共有鍵を生成する相手の電子メールアドレスにドメイン名が付いていなければ、共通鍵を正しく生成できなくなり、暗号通信を行うことができない。

【００５４】

そこで、図９（Ｉ）及び図９（II）に示すように、送信側となるエンティティａにおいて、相手先として指定されたエンティティｂの電子メールアドレスにドメイン名が付いていない場合には（Ｓ４１１）、エンティティａと同じドメイン名を付けて（Ｓ４１２）、共通鍵K_{ab}の生成を行うようにした（Ｓ４１３）。

【００５５】

また、受信側となるエンティティｂにおいて、エンティティａから受信した電子メールの発信元情報（Ｆｒｏｍフィールド）等の電子メールアドレスに、ドメイン名が付いていない場合には（Ｓ４２１）、エンティティｂと同じドメイン名を付けて（Ｓ４２２）、共通鍵K_{ba}の生成を行うようにした（Ｓ４２３）。

【００５６】

（エンティティａにおける暗号化処理、エンティティｂにおける復号処理）

図７に戻り、エンティティａにあって、共通鍵生成部１５で生成された共通鍵K_{ab}を用いて、平文暗号化部１６にて、平文（メッセージ）Ｍが暗号文Ｃに暗号化されて（Ｓ３１３）、その暗号文Ｃが電子メールによる通信路３０へ送信される（Ｓ３１４）。エンティティｂにあって、共通鍵生成部２５で生成された共通鍵K_{ba}を用いて、暗号文復号部２６にて、暗号文Ｃが元の平文（メッセージ）Ｍに復号される（Ｓ３２４）。

【００５７】

図１０は、本発明の記録媒体の実施例の構成を示す図である。ここに例示するプログラムは、秘密鍵の発行をセンタへ依頼する登録処理、各エンティティからの依頼に基づいて各センタにおいて各エンティティ固有の秘密鍵を発行する上述したような秘密鍵発行処理、各センタから秘密鍵方式で発行された秘密鍵を各エンティティにおいて復号する上述したような秘密鍵復号処理、自身固有の秘密鍵を用いて通信相手との間の共通鍵を生成する上述したような共通鍵作成処理、センタの秘密情報（対称行列）、各エンティティの秘密鍵（秘密鍵ベクトル）を暗号化して格納する上述したような秘密情報、秘密鍵の格納・更新処理、共通鍵、平文、暗号文を表示する上述したような表示処理、及び／または、平文の暗号化処理、暗号文の復号処理等を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各ホスト側または各エンティティ側に設けられている。

【００５８】

図１０において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、少なくとも１つの上記処理を実行する。

【００５９】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭ等を用いてなり、記録媒体４２には前述の如きプルグラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、少なくとも１つの上記処理を実行する。

【００６０】

コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク、ＣＤ－ＲＯＭまたはフレキシブルディスク等を用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピュ

ータ４０を制御することにより、少なくとも１つ以上の上記処理を実行する。

【００６１】

【発明の効果】

以上詳述したように、本発明では、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、自身の電子メールアドレスのドメイン名と同じドメイン名を、相手の電子メールアドレスに付けてから共通鍵を生成するようにした。操作ミスやメールシステムにより、通信相手の電子メールアドレスにドメイン名が付かないような場合でも、共通鍵を生成することができる。

【図面の簡単な説明】

【図１】

本発明の暗号通信システムの構成を示す模式図である。

【図２】

２個のエンティティ間における情報の通信状態を示す模式図である。

【図３】

秘密鍵発行器の内部構成を示す図である。

【図４】

エンティティのＩＤベクトル（特定情報）分割例を示す模式図である。

【図５】

エンティティにおける登録処理を示す流れ図である。

【図６】

エンティティにおける登録処理及びセンタにおける秘密鍵発行処理を示す流れ図である。

【図７】

エンティティ間における共通鍵生成及処理、暗号化処理及び復号処理を示す流れ図である。

【図８】

電子メールアドレスの例を示す図である。

【図９】

共通鍵生成処理を示す流れ図である。

【図１０】

記録媒体の実施例の構成を示す図である。

【図１１】

ＩＤ－ＮＩＫＳのシステムの原理構成図である。

【符号の説明】

１　センタ

２　秘密鍵発行器

５　秘密鍵生成部

１０，２０　秘密鍵登録部

１５，２５　共通鍵生成部

１６　平文暗号化部

２６　暗号文復号部

３０　通信路

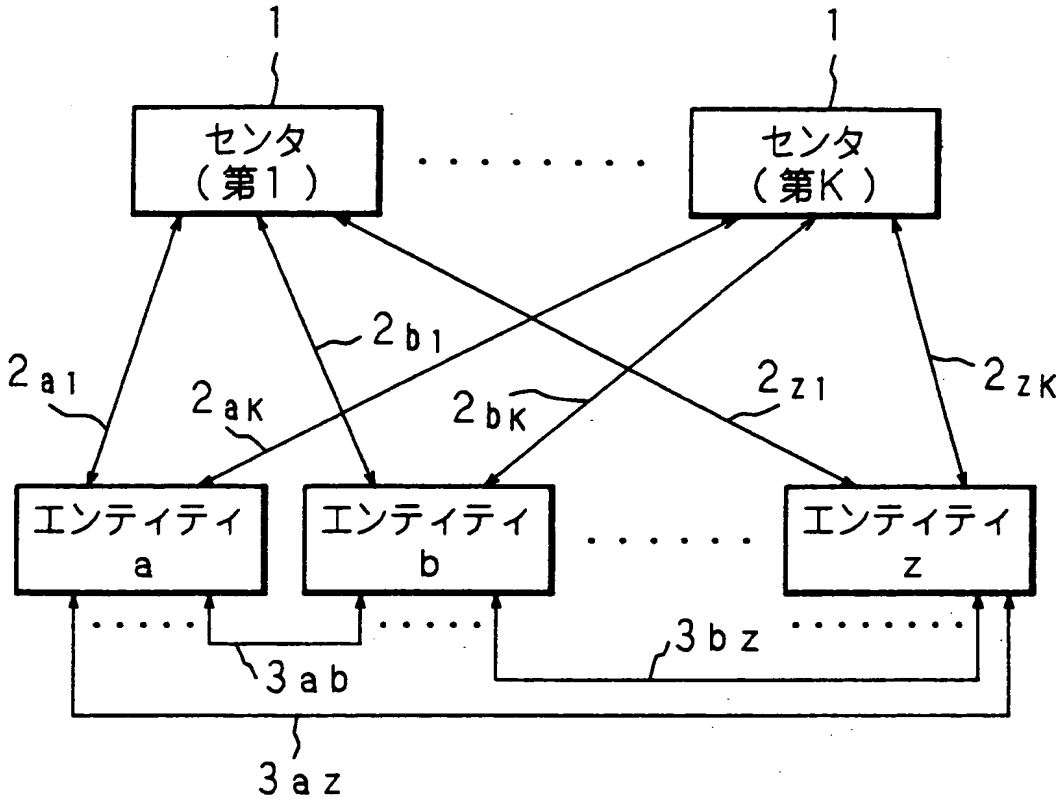
４０　コンピュータ

４１，４２，４３　記録媒体

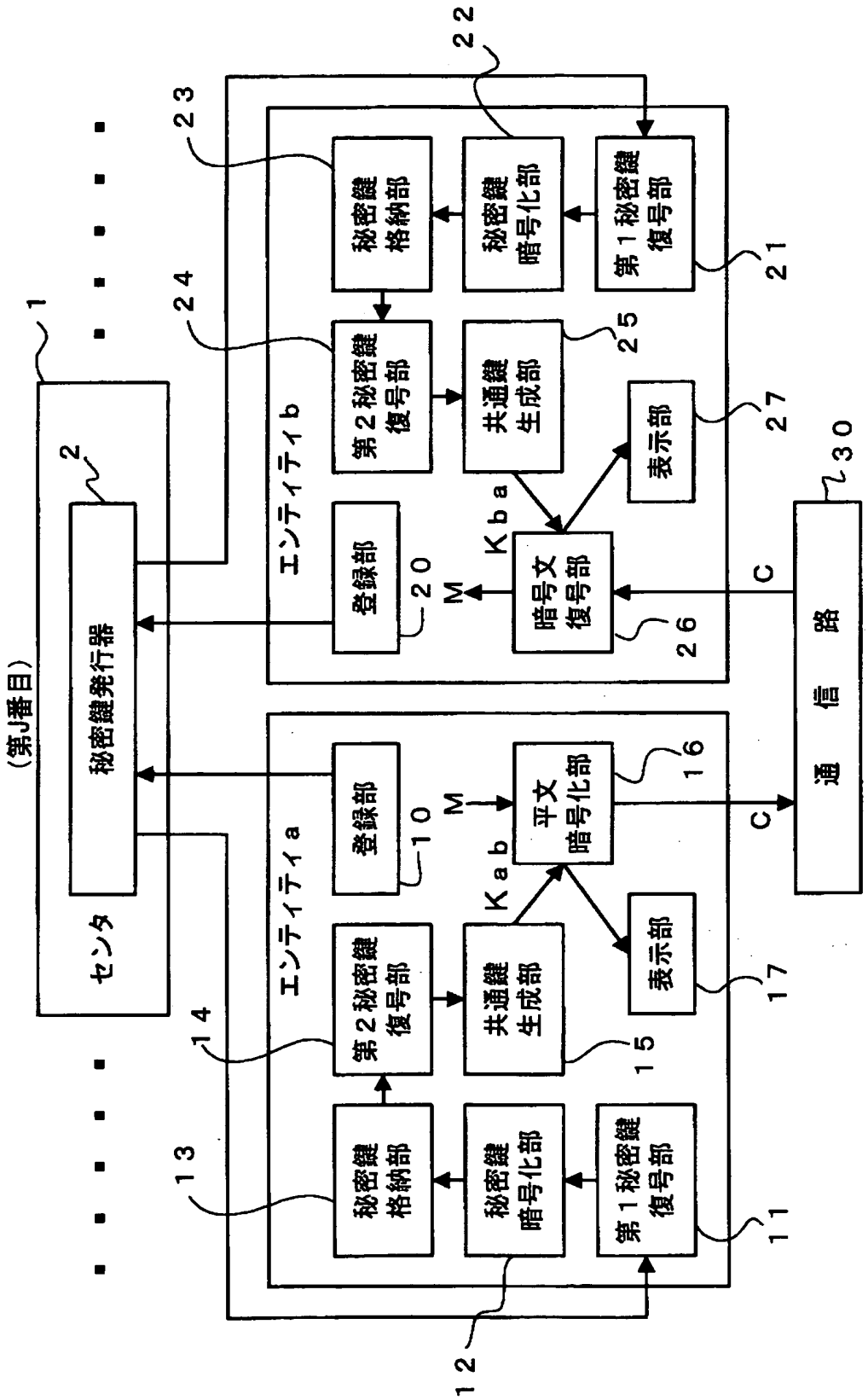
ａ，ｂ，ｚ　エンティティ

【書類名】　　図面

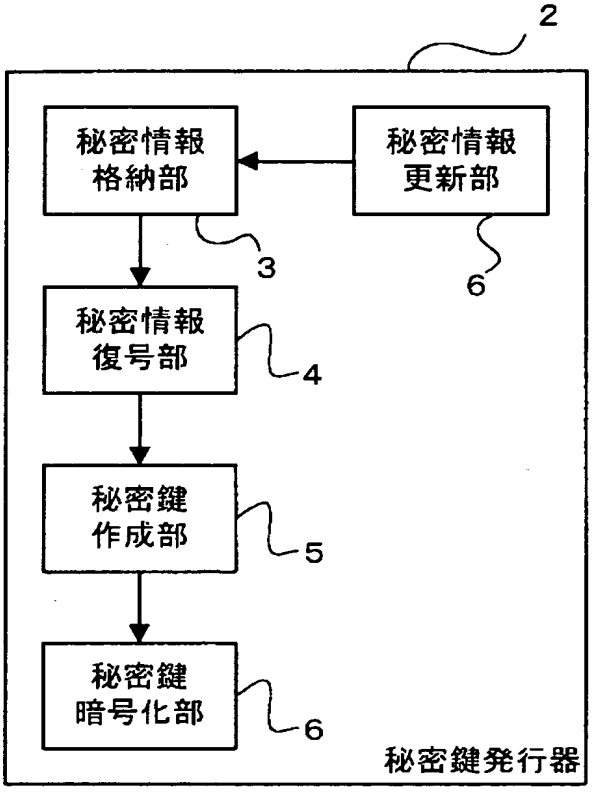
【図１】


1
1
センタ
（第1）
センタ
（第K）
2a1
2aK
2b1
2bK
2z1
2zK
エンティティ
a
エンティティ
b
エンティティ
z
3ab
3bz
3az

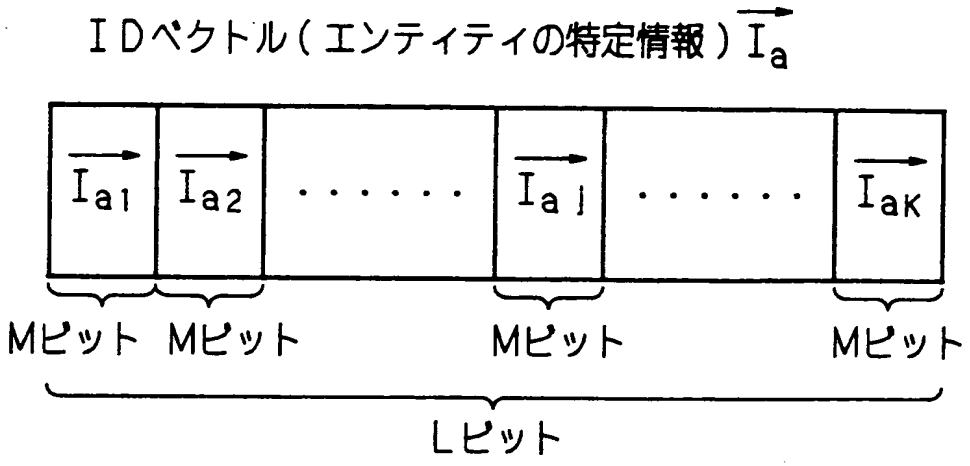
【図２】


(第J番目)
センタ
秘密鍵発行器
2
1
エンティティa
登録部
10
M
Kab
平文暗号化部
16
C
通信路
30
表示部
17
共通鍵生成部
15
第２秘密鍵復号部
14
秘密鍵暗号化部
13
秘密鍵格納部
12
第１秘密鍵復号部
11
エンティティb
登録部
20
M
Kba
暗号文復号部
26
C
表示部
27
共通鍵生成部
25
第２秘密鍵復号部
24
秘密鍵暗号化部
23
秘密鍵格納部
22
第１秘密鍵復号部
21

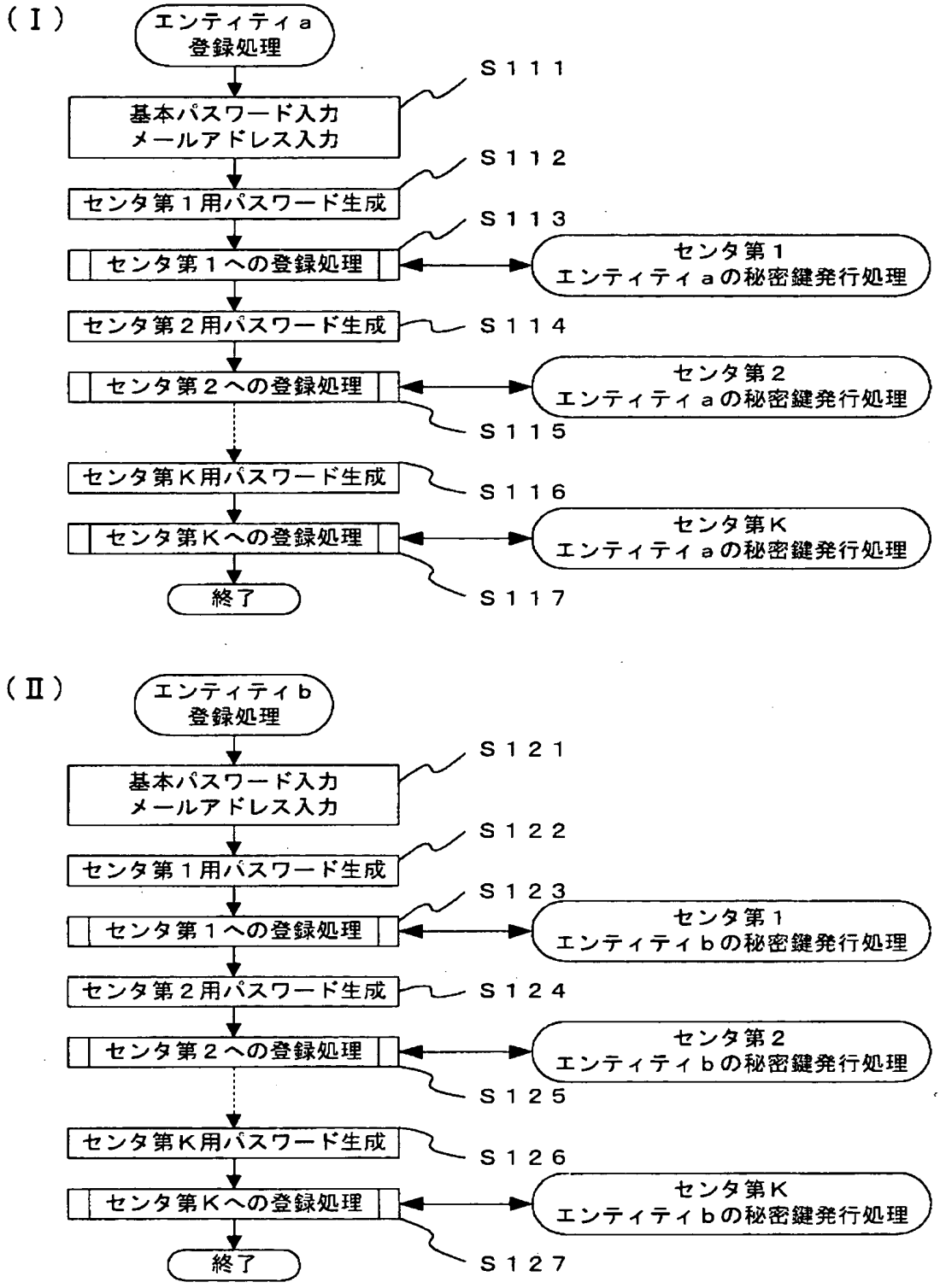
【図３】



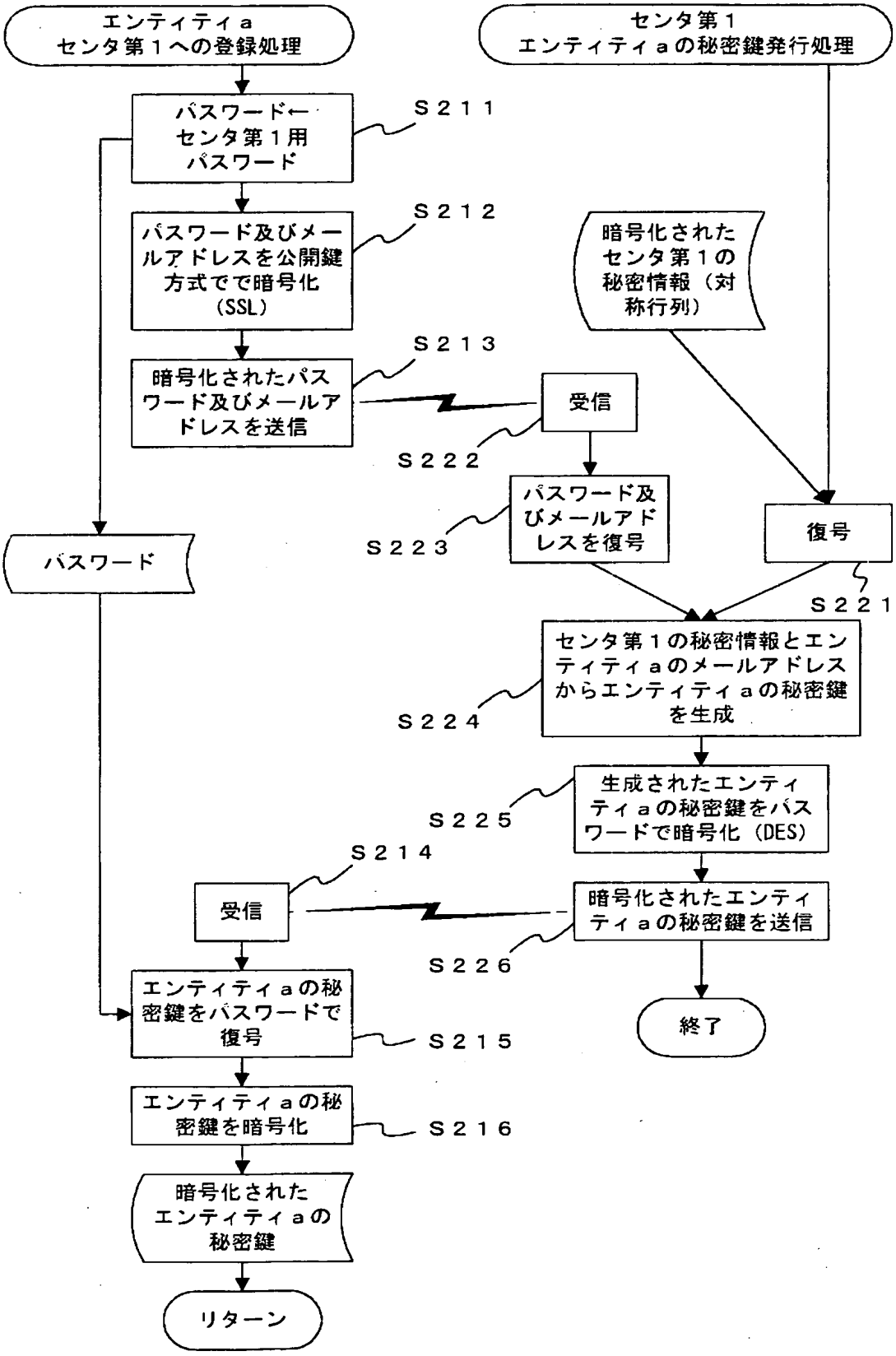
【図４】


IDベクトル（エンティティの特定情報）$\vec{I_a}$
$\vec{I_{a1}}$
$\vec{I_{a2}}$
$\vec{I_{aj}}$
$\vec{I_{aK}}$
Mビット
Mビット
Mビット
Mビット
Lビット

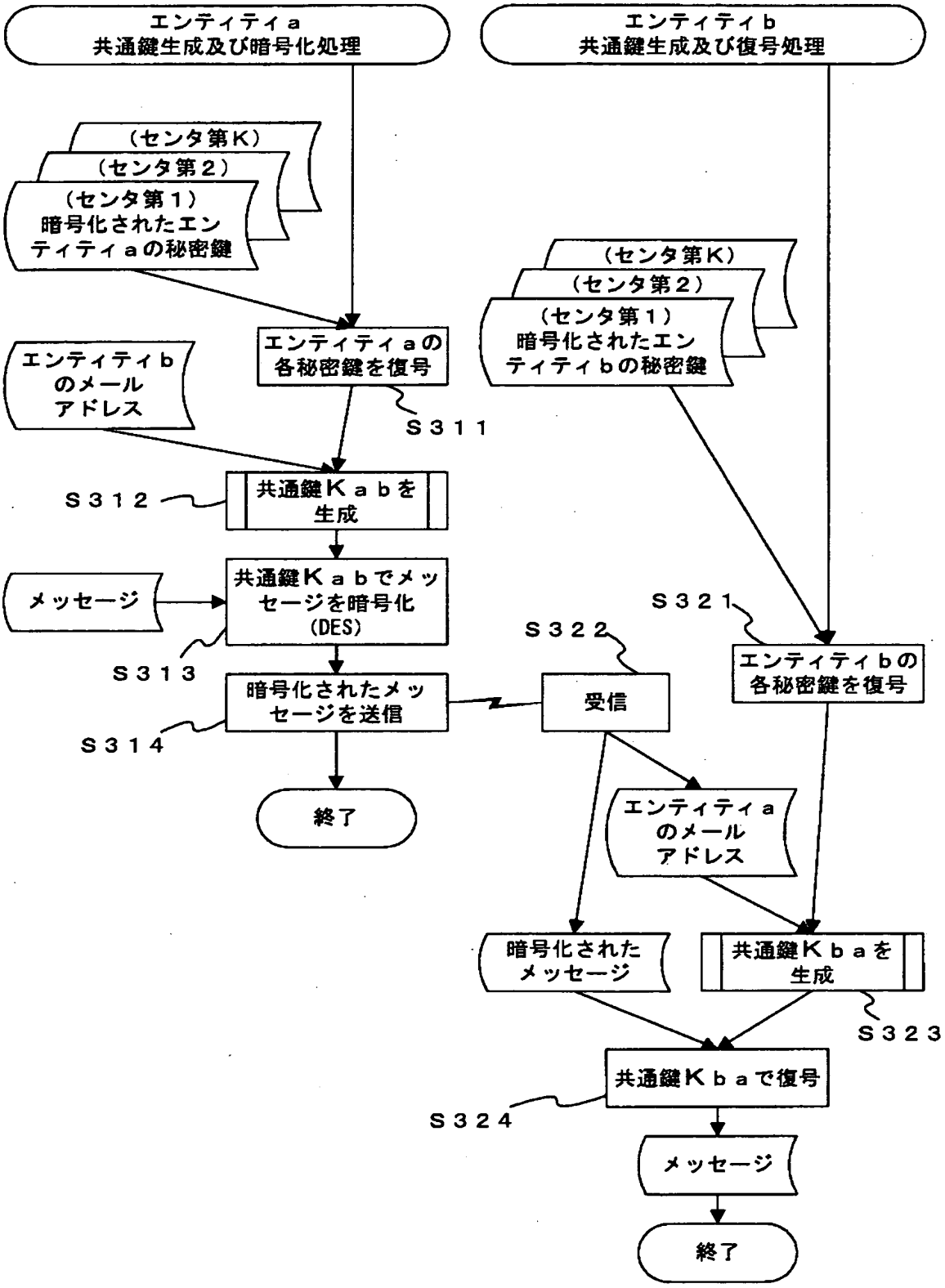
【図５】


（Ⅰ）
エンティティａ
登録処理
Ｓ１１１
基本パスワード入力
メールアドレス入力
Ｓ１１２
センタ第１用パスワード生成
Ｓ１１３
センタ第１への登録処理
センタ第１
エンティティａの秘密鍵発行処理
センタ第２用パスワード生成
Ｓ１１４
センタ第２への登録処理
センタ第２
エンティティａの秘密鍵発行処理
Ｓ１１５
センタ第Ｋ用パスワード生成
Ｓ１１６
センタ第Ｋへの登録処理
センタ第Ｋ
エンティティａの秘密鍵発行処理
終了
Ｓ１１７
（Ⅱ）
エンティティｂ
登録処理
Ｓ１２１
基本パスワード入力
メールアドレス入力
Ｓ１２２
センタ第１用パスワード生成
Ｓ１２３
センタ第１への登録処理
センタ第１
エンティティｂの秘密鍵発行処理
センタ第２用パスワード生成
Ｓ１２４
センタ第２への登録処理
センタ第２
エンティティｂの秘密鍵発行処理
Ｓ１２５
センタ第Ｋ用パスワード生成
Ｓ１２６
センタ第Ｋへの登録処理
センタ第Ｋ
エンティティｂの秘密鍵発行処理
終了
Ｓ１２７

【図６】


エンティティａ
センタ第１への登録処理
センタ第１
エンティティａの秘密鍵発行処理
パスワード←
センタ第１用
パスワード
Ｓ２１１
パスワード及びメール
アドレスを公開鍵
方式でで暗号化
（SSL）
Ｓ２１２
暗号化された
センタ第１の
秘密情報（対
称行列）
暗号化されたパス
ワード及びメールア
ドレスを送信
Ｓ２１３
受信
Ｓ２２２
パスワード及
びメールアド
レスを復号
Ｓ２２３
パスワード
復号
Ｓ２２１
センタ第１の秘密情報とエン
ティティａのメールアドレス
からエンティティａの秘密鍵
を生成
Ｓ２２４
生成されたエンティ
ティａの秘密鍵をパス
ワードで暗号化（DES）
Ｓ２２５
Ｓ２１４
受信
暗号化されたエンティ
ティａの秘密鍵を送信
Ｓ２２６
エンティティａの秘
密鍵をパスワードで
復号
Ｓ２１５
終了
エンティティａの秘
密鍵を暗号化
Ｓ２１６
暗号化された
エンティティａの
秘密鍵
リターン

【図７】


エンティティａ
共通鍵生成及び暗号化処理
エンティティｂ
共通鍵生成及び復号処理
（センタ第Ｋ）
（センタ第２）
（センタ第１）
暗号化されたエンティティａの秘密鍵
エンティティａの各秘密鍵を復号
Ｓ３１１
エンティティｂのメールアドレス
Ｓ３１２
共通鍵Ｋａｂを生成
メッセージ
共通鍵Ｋａｂでメッセージを暗号化（DES）
Ｓ３１３
暗号化されたメッセージを送信
Ｓ３１４
終了
（センタ第Ｋ）
（センタ第２）
（センタ第１）
暗号化されたエンティティｂの秘密鍵
Ｓ３２１
エンティティｂの各秘密鍵を復号
Ｓ３２２
受信
エンティティａのメールアドレス
暗号化されたメッセージ
共通鍵Ｋｂａを生成
Ｓ３２３
共通鍵Ｋｂａで復号
Ｓ３２４
メッセージ
終了

【図８】

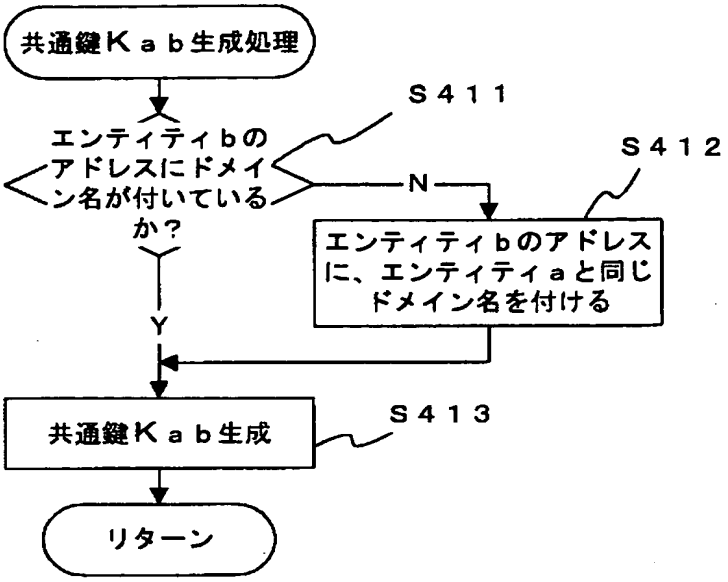
メールアドレスの例

（Ｉ）ドメイン名が付いている場合　　thomas@xyz.co.jp
ドメイン名

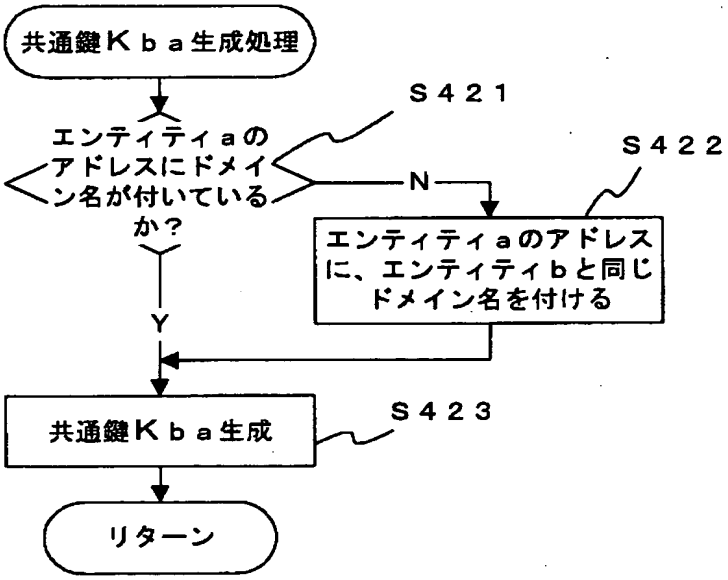
（Ⅱ）ドメイン名が付いていない場合　　thomas

【図９】

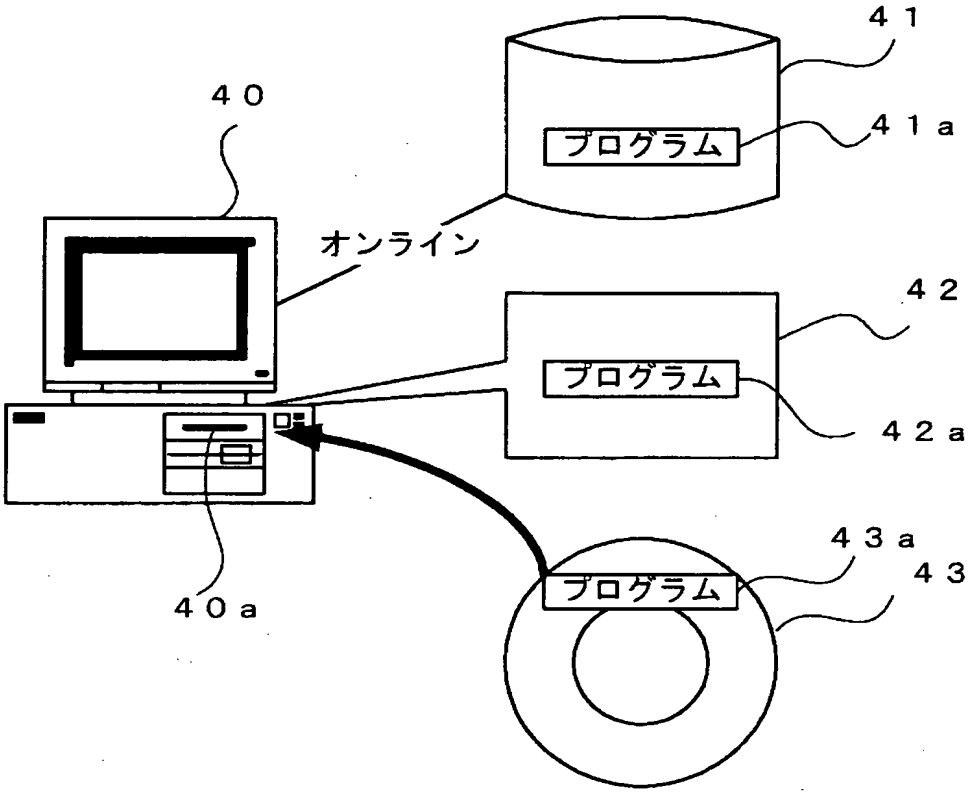
（Ｉ）


共通鍵Ｋａｂ生成処理
Ｓ４１１
エンティティｂのアドレスにドメイン名が付いているか？
Ｎ
Ｓ４１２
エンティティｂのアドレスに、エンティティａと同じドメイン名を付ける
Ｙ
共通鍵Ｋａｂ生成
Ｓ４１３
リターン

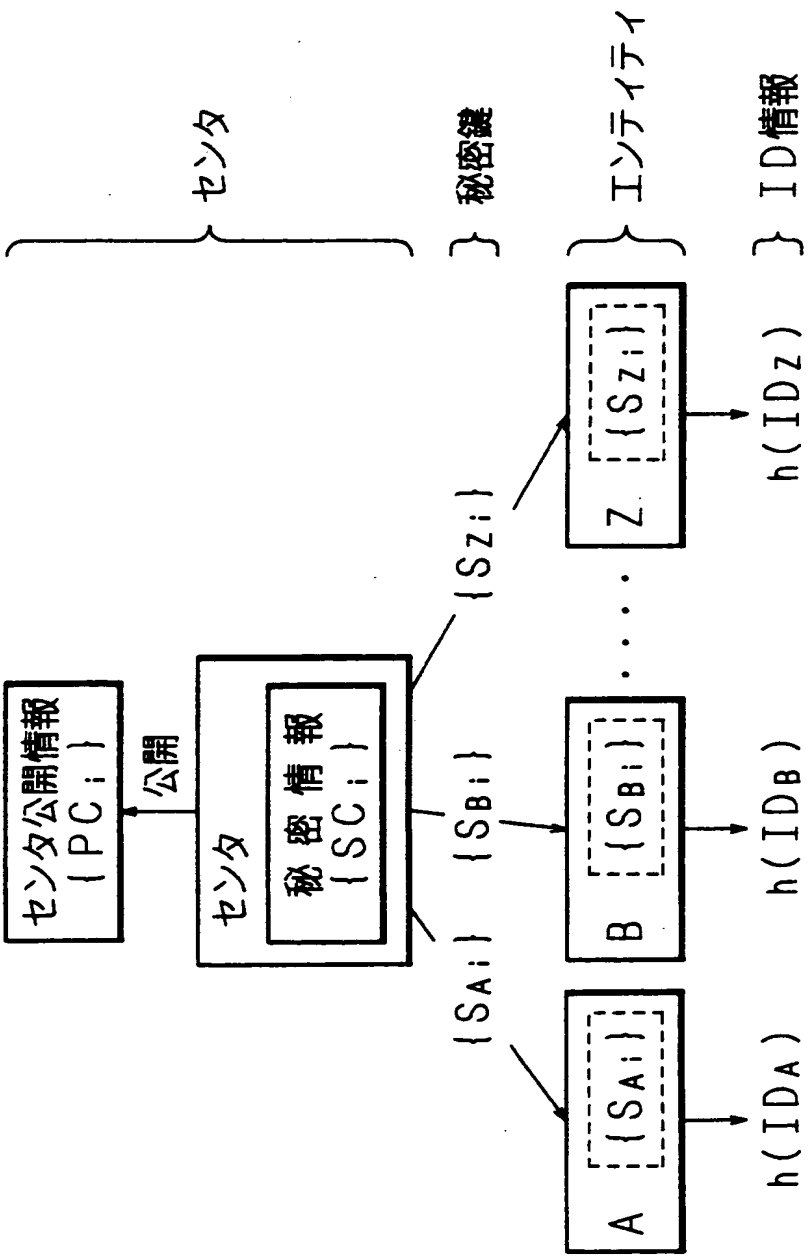
（Ⅱ）


共通鍵Ｋｂａ生成処理
Ｓ４２１
エンティティａのアドレスにドメイン名が付いているか？
Ｎ
Ｓ４２２
エンティティａのアドレスに、エンティティｂと同じドメイン名を付ける
Ｙ
共通鍵Ｋｂａ生成
Ｓ４２３
リターン

【図１０】



【図１１】


センタ
秘密鍵
エンティティ
ID情報
センタ公開情報
{PCi}
公開
センタ
秘密情報
{SCi}
{SZi}
{SBi}
{SAi}
Z
{SZi}
B
{SBi}
A
{SAi}
h(IDZ)
h(IDB)
h(IDA)

【書類名】　　要約書

【要約】

【課題】　ＩＤ－ＮＩＫＳにおいて、ＩＤ情報として電子メールアドレスを使用した場合に、確実な共通鍵生成を行う。

【解決手段】　各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、共通鍵を正しく生成できないので、自身の電子メールアドレスのドメイン名と同じドメイン名を、相手の電子メールアドレスに付けてから共通鍵を生成するようにした。

【選択図】　　図９

認定・付加情報

特許出願の番号	特願２０００－０１６３６２
受付番号	５００００７３７４２
書類名	特許願
担当官	宇留間　久雄　　７２７７
作成日	平成１２年　６月１５日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000006297
- 【住所又は居所】 京都府京都市南区吉祥院南落合町３番地
- 【氏名又は名称】 村田機械株式会社

【特許出願人】
- 【識別番号】 597008636
- 【住所又は居所】 大阪府箕面市粟生外院４丁目１５番３号
- 【氏名又は名称】 笠原　正雄

【復代理人】
- 【識別番号】 100114557
- 【住所又は居所】 大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】 河野　英仁

【代理人】 申請人
- 【識別番号】 100078868
- 【住所又は居所】 大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】 河野　登夫

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄